# ETSI TS 132 593 V19.0.0 (2025-10)

TECHNICAL SPECIFICATION

**LTE;**
**Telecommunication management;**
**Home enhanced Node B (HeNB) Operations, Administration, Maintenance and Provisioning (OAM&P);**
**Procedure flows for Type 1 interface**
**HeNB to HeNB Management System (HeMS)**
**(3GPP TS 32.593 version 19.0.0 Release 19)**

Reference
RTS/TSGS-0532593vj00

Keywords
LTE

***ETSI***

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

# Intellectual Property Rights

## Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

## Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

# Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found at 3GPP to ETSI numbering cross-referencing.

# Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

# Contents

# Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

# Introduction

The present document is part of a TS-family covering the 3rd Generation Partnership Project Technical Specification Group Services and System Aspects, Telecommunication Management; as identified below:

3GPP TS 32.591: "Telecommunications management; Home eNode B (HeNB) Operations, Administration, Maintenance and Provisioning (OAM&P); Concepts and requirements for Type 1 interface HeNB to HeNB Management System".

3GPP TS 32.592: "Telecommunications management; Home eNode B (HeNB) Operations, Administration, Maintenance and Provisioning (OAM&P); Information model for Type 1 interface HeNB to HeNB Management System".

**3GPP TS 32.593: "Telecommunications management; Home Node B (HeNB) Operations, Administration, Maintenance and Provisioning (OAM&P); Procedure flows for Type 1 interface HeNB to HeNB Management System ".**

3GPP TS 32.594: "Telecommunications management; Home eNode B (HeNB) Operations, Administration, Maintenance and Provisioning (OAM&P); XML definitions for Type 1 interface HeNB to HeNB Management System".

# 1 Scope

The present specification describes the procedure flows between network entities involved in HeNB management-related tasks. These procedures are based on the requirements specified in [4]. Information model for management-related information exchanged in these procedures is specified in [5] and references therein. XML file formats used to encapsulate the information exchanged in these procedures are specified in [6]. The communication protocol used for HeNB management is the TR-069 protocol, specified in [7].

Management interface affected by these procedures is the Type 1 interface between HeNB and HeMS. Procedures flows over the Type 2 interface (between Element Management and Network Management layer) for the management of HeNB are outside of scope of this document

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 32.101: "Telecommunication management; Principles and high level requirements".

[3] 3GPP TS 32.102: "Telecommunication management; Architecture".

[4] 3GPP TS 32.591: "Telecommunications management; Home eNode B (HeNB) Operations, Administration, Maintenance and Provisioning (OAM&P); Concepts and Requirements for Type 1 interface HeNB to HeNB Management System".

[5] 3GPP TS 32.592: "Telecommunications management; Home eNode B (HeNB) Operations, Administration, Maintenance and Provisioning (OAM&P); Information model for Type 1 interface HeNB to HeNB Management System".

[6] 3GPP TS 32.594: "Telecommunications management; Home eNode B (HeNB) Operations, Administration, Maintenance and Provisioning (OAM&P); XML definitions for Type 1 interface HeNB to HeNB Management System".

[7] TR-069 Amendment 2, CPE WAN Management Protocol v1.1, Broadband Forum, viewable at http://www.broadband-forum.org/technical/download/TR-069Amendment2.pdf.

[8] 3GPP TS 36.413: " Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)".

[9] 3GPP TS 33.320: "Security of Home Node B (HNB) / Home evolved Node B (HeNB)".

# 3 Definitions and Abbreviations

For the purposes of the present document, the terms and definitions given in TS 32.101 [2], TS 32.102 [3] and TS 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TS 32.101 [2], TS 32.102 [3] and TS 21.905 [1], in that order.

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

## 3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

| | |
|---|---|
| CM | Configuration Management |
| DNS | Domain Name Server |
| EPC | Evolved Packet Core |
| FM | Fault Management |
| FQDN | Fully Qualified Domain Name |
| FTP | File Transfer Protocol |
| HMS | Home NodeB Management System |
| HeMS | Home eNodeB Management System |
| HNB | Home NodeB |
| HeNB | Home eNodeB |
| HeNB-GW | HeNB Gateway |
| HTTP | Hyper Text Transfer Protocol |
| HTTPS | Hyper Text Transfer Protocol Secure |
| IP | Internet Protocol |
| LAN | Local Area Network |
| MME | Mobility Management Entity |
| MNO | Mobile Network Operator |
| OAM | Operation, Administration, Maintenance |
| PM | Performance Management |
| RPC | Remote Procedure Call |
| SeGW | Security Gateway |
| SSL | Secure Socket Layer |
| SFTP | Secure File Transfer Protocol |
| TLS | Transport Layer Security |

# 4 Architecture for HeNB Management

## 4.1 HeNB OAM Functional Architecture

### 4.1.1 Overview

This section describes the functional architecture for HeNB management over Type 1 management interface and entities involved.

The architecture is shown in Figure 4-1 Functionalities of each entity are described in subsequent subclauses. Non-OAM entities, such as SeGW and MME are also shown as they figure in the procedure flows specified in this document.

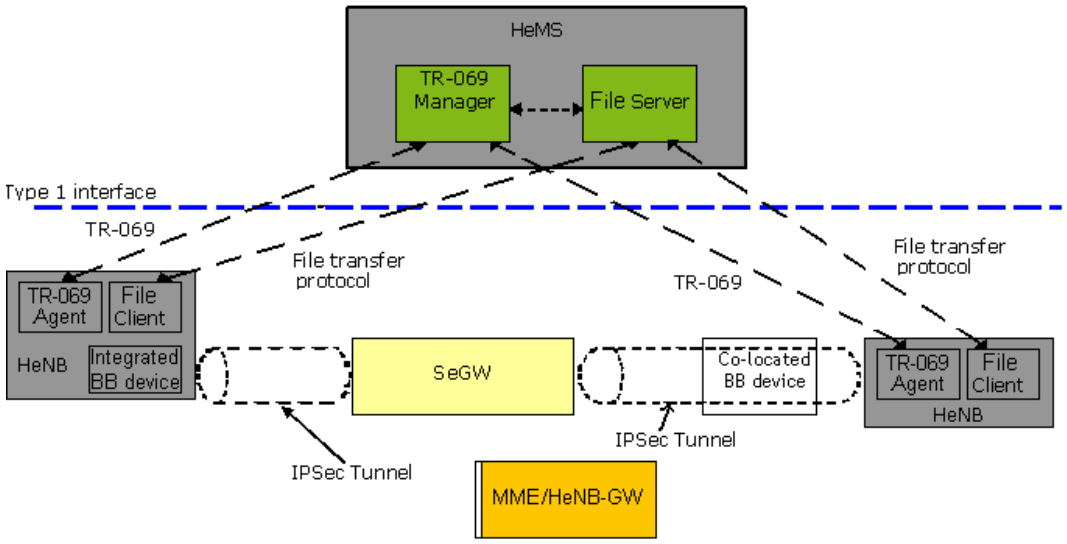


**Figure 4-1: HeNB Management Architecture**

# 4.2 Functional Elements

## 4.2.1 HeNB Management System (HeMS)

The HeMS supports the procedures for:

- Configuration Management (CM), Fault management (FM) and Performance Management (PM) of HeNB
- Identity and location verification of HeNB
- Discovery and assignment of Serving HeMS, Serving SeGW, and MME
- File upload/download related to HeNB management.

The HeMS comprises a TR-069 Manager and an file server.

The TR-069 Manager corresponds to the TR-069 Auto-Configuration Server (ACS) function as defined in TR-069 specification [7].

The file server may be used for file upload or download related to HeMS management, such as upload of performance measurement files or alarm logs, as configured by TR-069 Manager. The file server may also be used for other purposes by network operator.

Typically, HeMS assumes one of the following two roles:

- Initial HeMS (subclause x.y.z.w)
- Initial Serving HeMS (subclause x.y.z.w)

### 4.2.1.1 Initial HeMS

The Initial HeMS may be used to perform identity and location verification of HeNB and assign appropriate Serving HMS, Security Gateway and MME to HeNB. The FQDN of the Initial HeMS may be factory programmed in the HeNB.

### 4.2.1.2 Serving HeMS

Serving HeMS supports the procedures for CM/FM/PM, file upload/download, and identity verification of the HeNB. Serving HeMS may also support MME discovery and assignment by HeNB.

Typically, Serving HeMS is located inside the operator's secure network domain and the address of the Serving HeMS is provided to the HeNB via Initial HeMS.

### 4.2.2 Home eNB

The HeNB is the managed device.

The HeNB logically comprises a TR-069 Agent and an file client.

TR-069 Agent corresponds to the TR-069 Customer Premise Equipment (CPE) function as defined in TR-069 specification [7].

The file client may be used for file upload or download related to HeMS management, such as upload of performance measurement files or alarm logs, as configured by TR-069 Manager via TR-069 Agent. The file client may also be used for other purposes not related to HeNB management.

HeNB is associated with a Broadband (BB) device. This is typically a residential gateway providing transport layer connectivity via an access provider domain. The BB device provides routing, NAT and firewall functionality. As shown in Figure 4-1, HeNB can be connected to an external BB device or a BB device can be integrated with the HeNB.

### 4.2.3 Security Gateway (SeGW)

SeGW provides authentication of HeNB secure tunnelling of communication between HeNB and HeMS and between HeNB and MME.

#### 4.2.3.1 Initial SeGW

Initial SeGW terminates IPSec and provides secure tunnelling of communication between HeNB and Initial HeMS. The FQDN of the Initial SeGW may be factory programmed in the HeNB. Initial SeGW can be the same as the Serving SeGW.

#### 4.2.3.2 Serving SeGW

Serving SeGW provides IPSec association and secure communication between HeNB and network elements such as MME and Serving HeMS in the operator's network. Serving SeGW implements a forwarding function to allow forwarding of IP packets upstream and downstream:

- Downstream: packets are forwarded on appropriate IPSec tunnels towards the HeNB based on their destination IP addresses;
- Upstream: forwarding IP traffic to the Serving HeMS, MME or other network elements based on destination IP addresses.

The FQDN of the Serving SeGW may be provided to the HeNB by Initial HeMS.

Serving SeGW could be the same as the Initial SeGW.

### 4.2.4 MME/HeNB GW

MME terminates S1 interface from HeNB. Optionally, S1 interface termination can be provided by HeNB Gateway. This is not relevant from the HeNB point of view, since HeNB cannot differentiate between connecting to MME and HeNBGW. From HeNB point of view, far-end S1 interface termination point appears as MME.

# 5 Procedure Flows

## 5.1 Discovery and Registration Procedures

### 5.1.1 Overview

When HeNB is powered up, it needs to establish connectivity with the Serving HeMS for management purposes and with the MME for EPC connectivity purposes. The transport layer protocol for both of these connections is IP. IP connectivity with Serving HeMS is established using Serving HeMS discovery procedures. Using these procedures, the HeNB is able to:

- Acquire IP address of the HeMS
- Establish secure IP connection with the HeMS

The IP address(es) of the S1 interface is provided to the HeNB in one of the following ways:

- By the Initial HeMS during Serving HeMS discovery procedure
- By the Serving HeMS during the registration procedure of the HeNB with the HeMS.

Once the HeNB has established the IP connectivity with the Serving HeMS, the HeNB must register with the Serving HeMS. This is accomplished using the HeNB registration with Serving HeMS procedure, described in clause 5.1.3.

The registration of the HeNB with MME (S1 Setup procedure) is specified in [8].

Figure 5-1 illustrates discovery and registration procedures executed by the HeNB upon power up.

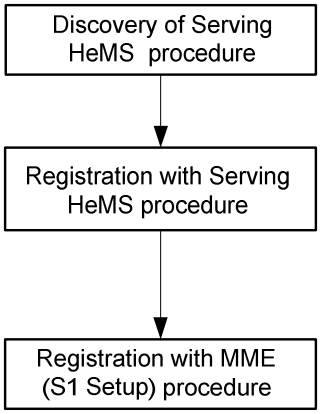


**Figure 5-1: Discovery and registration procedures**

### 5.1.2 Serving HeMS discovery procedures

#### 5.1.2.1 Overview

Operators may deploy their management infrastructure in different ways. Specifically, Initial HeMS may be accessible within the operator's secure public network domain or on the public internet. The following Serving HeMS discovery procedures are defined to accommodate these deployment scenarios:

- Serving HeMS discovery via Initial HeMS accessible inside operator's private secure network domain (clause 5.1.2.2)
- Serving HeMS discovery via Initial HeMS accessible on the public internet (clause 5.1.2.3).

#### 5.1.2.2 Serving HeMS Discovery via Initial HeMS accessible inside operator's private secure network domain (Conditional Mandatory)

This procedure applies for deployments where Initial HeMS is accessible only from inside the operator's private secure network domain, For such deployments the support for this procedure by HeNB is mandatory. Otherwise, the support for this procedure is not mandatory.

In this case the HeNB is factory programmed with:

- FQDN or IP address of the Initial HeMS
- FQDN or IP address of the Initial SeGW
- Operator trusted root CA certificate allowing the validation of the certificate presented by HeMS (as TLS server) or SeGW (as IKEv2 responder)

The address information (either FQDN or IP address) of Initial SeGW should be consistent with that in the certificate presented by Initial SeGW. When authentication between HeNB and Initial HeMS is needed, the address information of Initial HeMS should be consistent with that in the certificate presented by Initial HeMS.

The procedure for Serving HeMS discovery via Initial HeMS accessible inside operator's private secure network domain is described next and illustrated in Figure 5-2.

As a pre-condition, the HeNB establishes IP connectivity to the Internet when it is initially powered up.

1. Steps 1.1-1.5 allow HeNB to establish a secure connection with the Intial HeMS.

   1.1 The HeNB initiates a process to get IP address of the Initial SeGW. If the HeNB already has the IP address then go to step 1.3. If the HeNB has the FQDN, the HeNB performs DNS query to a public DNS for the IP address corresponding to the FQDN of the Initial SeGW.

   1.2 DNS responds to the HeNB with the IP address of the Initial SeGW.

   1.3 A secure connection via IPSec tunnel is established between the HeNB and Initial SeGW.

   1.4 The HeNB initiates a process to get IP address of the Initial HeMS. If the HeNB already has the IP address then skip step 1.4 and step 1.5. If the HeNB has the FQDN, the HeNB performs DNS query to a private DNS for the IP address corresponding to the FQDN of the Initial HeMS.

   1.5 Private DNS responds to the HeNB with the IP address of the Initial HeMS.

   A secure connection via IPSec tunnel is now established between the HeNB and the Initial HeMS.

2. Steps 2.1-2.2 allow the HeNB to establish a TR-069 session with Initial HeMS, as specified in [7].

   2.1 The HeNB sends to Initial HeMS an Inform request containing Device ID of the HeNB and optionally location information and/or other parameters.

   2.2 Initial HeMS returns an InformResponse to accept the session.

3. Steps 3.1-3.2 allow the HeMS to provide the HeNB with the FQDN or the IP address of the Serving SeGW and Serving HeMS.

   3.1. Initial HeMS invokes SetParameterValues RPC method to configure the FQDN or the IP address of the Serving SeGW and Serving HeMS. The Initial HeMS must provide the identity of the Serving SeGW and Serving HeMS in exactly the form as contained in the server certificate (IP address or FQDN), as the HeNB will perform a match of the subject name in the certificate against this configured parameter. Initial HeMS may also provide the far-end IP address of the S1 interface at this stage. If the Initial HeMS does not provide the far-end IP address of the S1 interface the Serving HeMS should provide it during the procedure for registration of HeNB with Serving HeMS (clause 5.1.3).

   3.2. The HeNB acknowledges the received parameters using SetParameterValuesResponse RPC method.

4. The HeNB releases the TR-069 Session between the HeNB and Initial HeMS, according to the criteria specified in [7].

5. The IPSec tunnel association may be destroyed between the HeNB and Initial SeGW.

6. Steps 6.1 – 6.5 allow HeNB to establish a secure connection with the Serving HeMS.

   6.1 The HeNB initiates a process to get IP address of the Serving SeGW. If the HeNB already has the IP address then go to step 6.3. If the HeNB has the FQDN, the HeNB performs DNS query to a public DNS for the IP address corresponding to the FQDN of the Serving SeGW.

   6.2 DNS responds to the HeNB with the IP address of the Serving SeGW.

   6.3 A secure connection via IPSec tunnel is established between the HeNB and Serving SeGW.

   6.4 The HeNB initiates a process to get IP address of the Serving HeMS. If the HeNB already has the IP address then skip steps 6.4 and 6.5. If the HeNB has the FQDN, the HeNB performs DNS query to a public DNS for the IP address corresponding to the FQDN of the Serving HeMS.

   6.5 Private DNS responds to the HeNB with the IP address of the Serving HeMS.

   A secure connection via IPSec tunnel is established between the HeNB and the Serving HeMS.

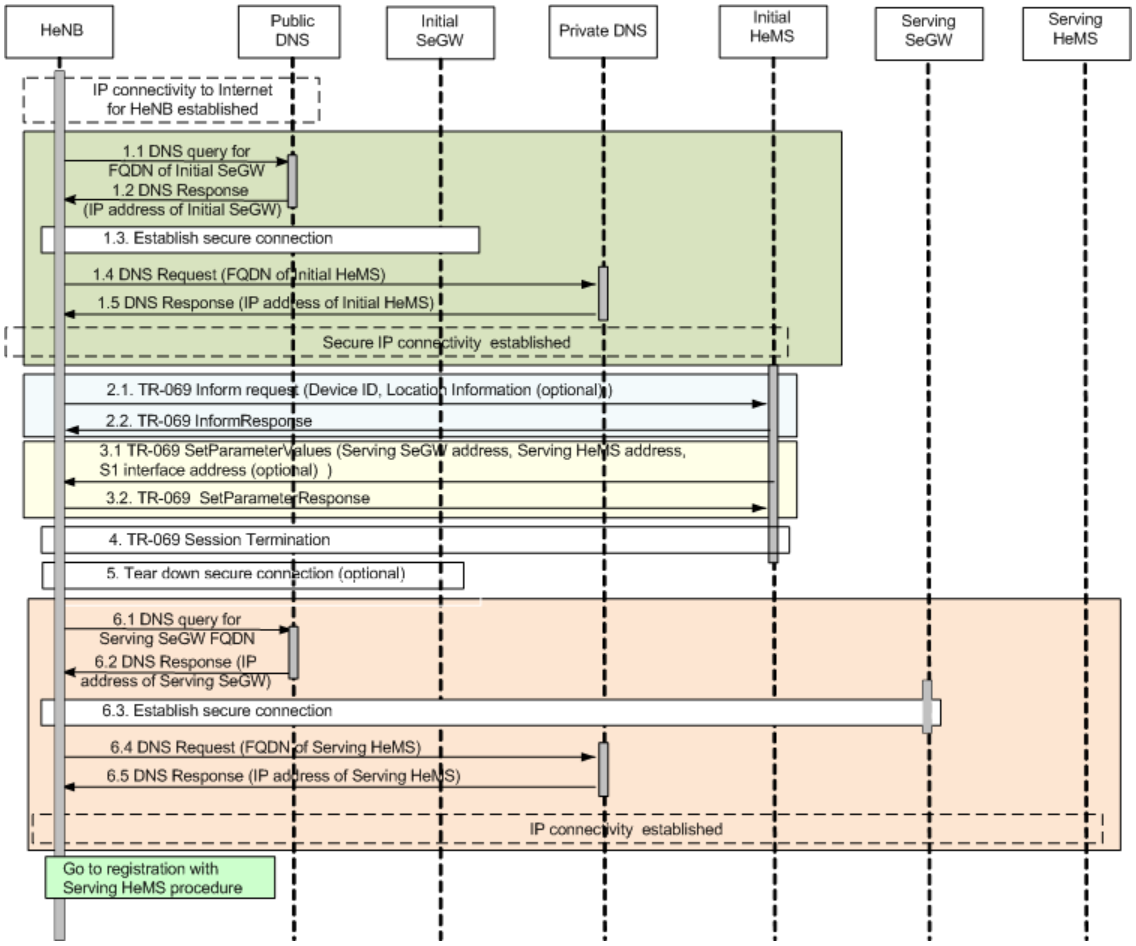


**Figure 5-2: Serving HeMS Discovery via Initial HeMS accessible inside operator's private secure network domain**

Next, the HeNB performs registration with the Serving HeMS procedure (clause 5.1.3).

### 5.1.2.3 Serving HeMS discovery via Initial HeMS accessible on the public internet (Conditional Mandatory)

This procedure applies for deployments where Initial HeMS is accessible on the public internet. In this case the HeNB is factory programmed with Initial HeMS' FQDN, which the operator needs to publish in a public DNS and with operator trusted root CA certificate allowing the validation of the certificate presented by HeMS (as TLS server). For such deployments, the support for this procedure by HeNB is mandatory. Otherwise, the support for this procedure is not mandatory.

The procedure for Serving HeMS discovery via Initial HeMS accessible on the public internet is described next and illustrated in Figure 5-3.

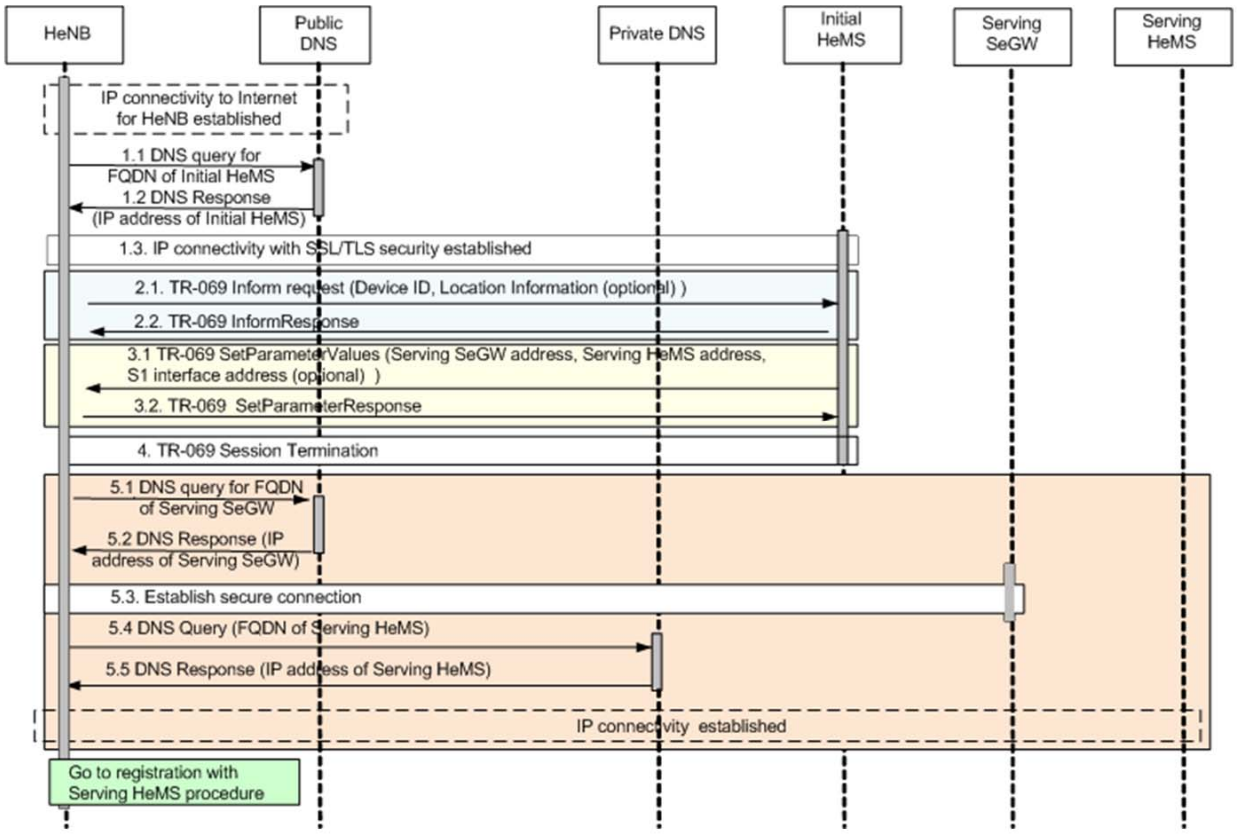


**Figure 5-3: Serving HeMS Discovery via Initial HeMS accessible on the public internet**

As a pre-condition, the HeNB establishes IP connectivity to the Internet when it is initially powered up.

1. In steps 1.1-1.3 HeNB establish IP connectivity with the Intial HeMS using SSL/TLS security. The HeNB must have a reference to the IP address of the Initial HeMS pre-programmed. The HeNB performs DNS query to a public DNS for the IP address corresponding to the FQDN of the Initial HeMS if needed.

   Steps 2 to 4 are identical to steps 2 to 4 in the procedure for Serving HeMS discovery via Initial HeMS accessible inside operator's private secure network domain (clause 5.1.2.2). Steps 5.1 to 5.5 are identical to steps 6.1 to 6.5 in the procedure for Serving HeMS discovery via Initial HeMS accessible inside operator's private secure network domain (clause 5.1.2.2).

   Next, the HeNB performs registration with the Serving HeMS (clause 5.1.3).

## 5.1.3 HeNB registration with Serving HeMS (Mandatory)

The procedure for HeNB registration with Serving HeMS is described next and illustrated in Figure 5-4.

As a pre-condition, the HeNB has discovered and establishes secure IP connectivity with the Serving HeMS. This is accomplished using appropriate Serving HeMS discovery procedure (clause 5.1.2).

1. Steps 1.1-1.2 allow the HeNB to establish a TR-069 session with Serving HeMS, as specified in [7].

   1.1 The HeNB sends to Serving HeMS an Inform request containing Device ID of the HeNB and optionally location information and/or other parameters.

   1.2 Serving HeMS returns an InformResponse to accept the session.

2. Steps 2.1-2.2 allow the HeMS to provide the HeNB with the far-end IP address of the S1 interface.

2.1 Serving HeMS invokes SetParameterValues RPC method to configure the far-end IP address of the S1 interface and optional IPsec usage indicator.

2.2. The HeNB acknowledges the received S1 interface IP address using SetParameterValuesResponse RPC method and optional IPsec usage indicator.

3. The HeNB may release the TR-069 Session between the HeNB and Serving HeMS, according to the criteria specified in [7].

4. The HeNB initiates the S1 Setup procedure (registration with MME) specified in [8].

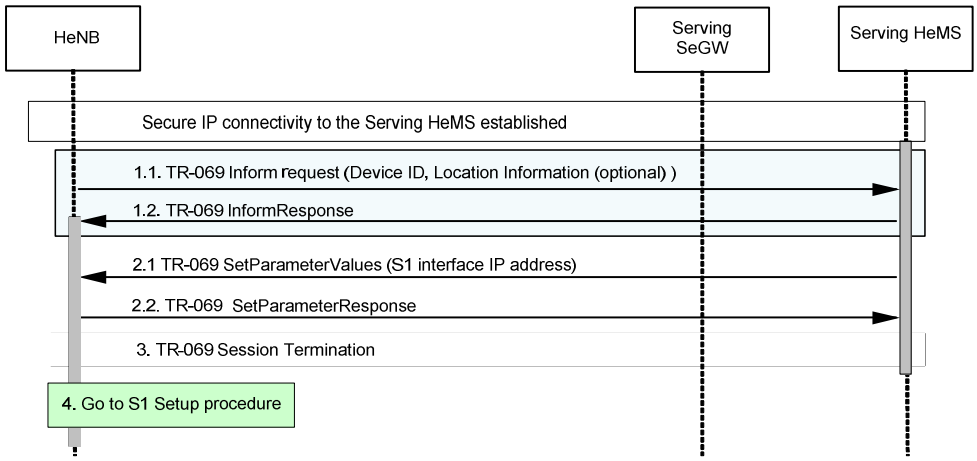


**Figure 5-4: Procedure for HeNB registration with Serving HeMS**

# 5.2 Configuration Management Procedures (Mandatory)

## 5.2.1 Overview

This section specifies the procedure flows for HeNB configuration management using TR-069 protocol specified in [7]. These procedure flows stem from the CM requirements in [4], which mandate that CM can be achieved either by means of TR-069 RPC methods as a mandatory feature or by means of file download as an optional feature.

The procedure for notification of the IPSec IP address change by the HeNB is also specified.

## 5.2.2 HeNB configuration using file download procedure (Optional)

Following a registration of the HeNB with the Serving HeMS, the TR-069 Manager in the Serving HeMS may trigger the HeNB to start a file download of configuration CM data. Subsequent to this initial phase, the TR-069 Manager may trigger this procedure at any time.

Procedure for HeNB configuration using file download is shown in Figure 5-5 and described next.

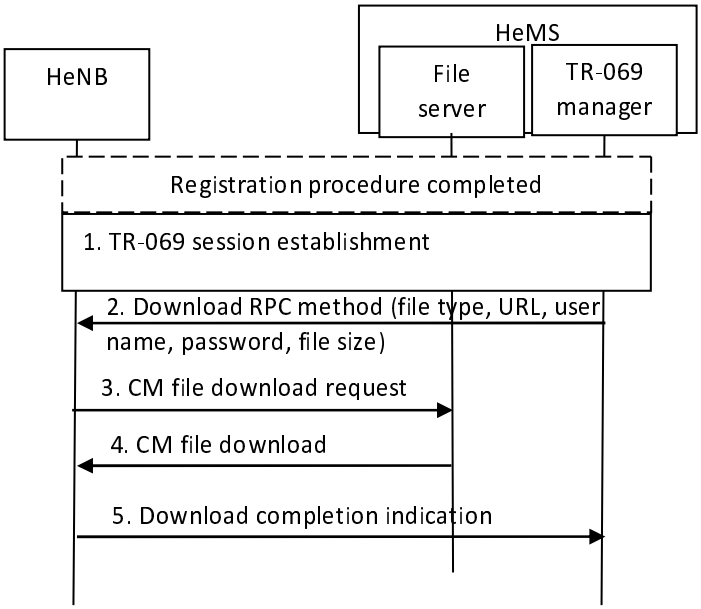


**Figure 5-5: HeNB configuration using file download procedure**

As a pre-condition, the HeNB must be registered with the HeMS.

1. The TR-069 session is established as described in [7].
2. HeMS invokes RPC method Download, specified in [7], to cause the HeNB to download a specified file from the designated location, which may be the file server in the HeMS as shown in Figure 5-5. The arguments of the Download RPC method are described in [7] and include:
   - File type,
   - URL specifying the source file location
   - User name for the connection to the file server
   - Password associated to the user name
   - File size

   Types and values of the arguments of the Download method are described in [7].
3. The HeNB initiates the file download using transport protocol inferred from the URL argument of the Download method.
4. The file server performs the file download. The file format is specified in [6].
5. The HeNB provides file download completion indication (success/unsuccessful) using the means described in [7]. The HeNB should indicate successful file download only after the new configuration has been successfully applied. In the case of download failure, none of the downloaded parameters shall be applied.

According to [7], TR-069 session may be terminated before or after the Download completion indication is sent by the HeNB.

The mechanisms by which the file is installed on the file server and the corresponding URL is built and provided to the TR-069 manager are not specified in this document.

### 5.2.3 HeNB configuration using SetParameterValues RPC method (Mandatory)

Procedure for HeNB configuration using TR-069 RPC method SetParameterValues is shown in Figure 5-6 and described next.

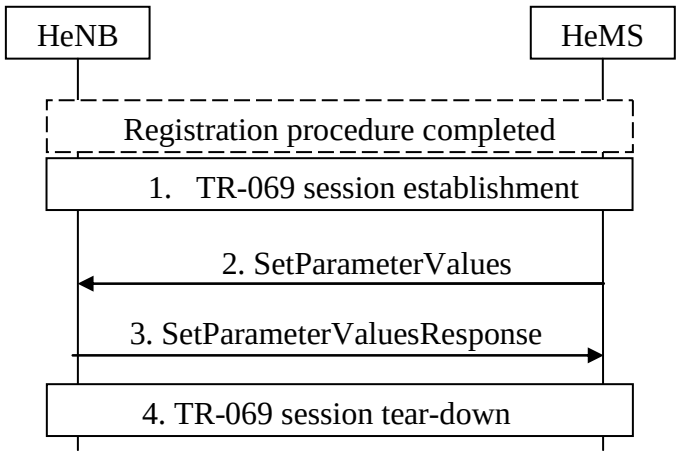


**Figure 5-6: HeNB configuration procedure using RPC SetParameterValues method**

As a pre-condition, the HeNB must be registered with the HeMS.

1. The TR-069 session is established as described in [7].
2. The HeMS invokes SetParameterValues RPC method, specified in [7], to configure the parameters in the HeNB. The arguments include the list of parameters to be configured and their values.
3. The HeNB sends SetParameterValueResponse with the Status argument. The type and values of this argument are described in [7]. The internal procedure that the HeNB must follow to:
   - apply new parameter values,
   - determine the value of the Status argument, and
   - send the SetParameterValueResponse

   is described in [7].
4. The TR-069 session may be torn down after SetParameterValueReponse is sent by the HeNB.

### 5.2.4 IPSec tunnel IP address change notification procedure (Conditional Mandatory)

The precondition is to configure HeNB using IPsec. If the inner IPsec tunnel IP address of the HeNB changes and HeNB is connected to HeMS via IPSec Tunnel then the HeNB shall notify the HeMS about the change of the IPSec IP address. To this end the HeNB shall establish a TR-069 session to the Serving HeMS and use the Inform method to update the IPSec tunnel IP address. The procedure is shown in Figure 5-7 and described next.

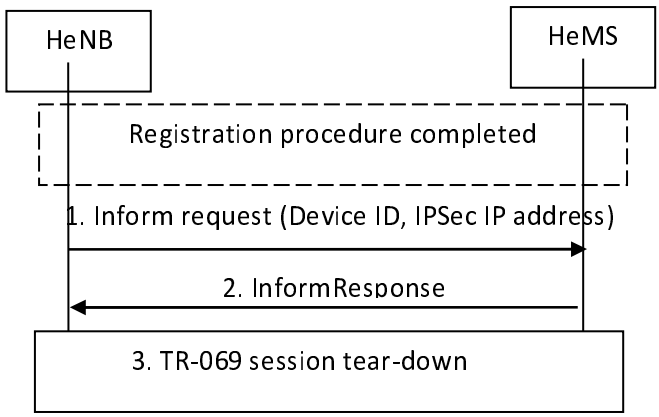


**Figure 5-7: IP address change notification procedure**

As a pre-condition, the HeNB must be registered with the HeMS.

1. The HeNB invokes Inform RPC method as soon as possible following a change of the IPSec IP address. In the arguments of the Inform method the HeNB shall include Device ID and the new IPSec IP address of the HeNB.
2. The HeMS acknowledges the receipt of the new IPSec IP address of the HeNB using InformResponse method.

The TR-069 session may be torn down.

## 5.3 Alarm Reporting Procedures

### 5.3.1 Alarm reporting mechanism configuration

This procedure allows TR-069 Manager, using SetParameterValues method, to select alarm attributes (such as perceived severity, alarm type) that HeNB shall use to classify its alarms for purpose of reporting them to TR-069 Manager.

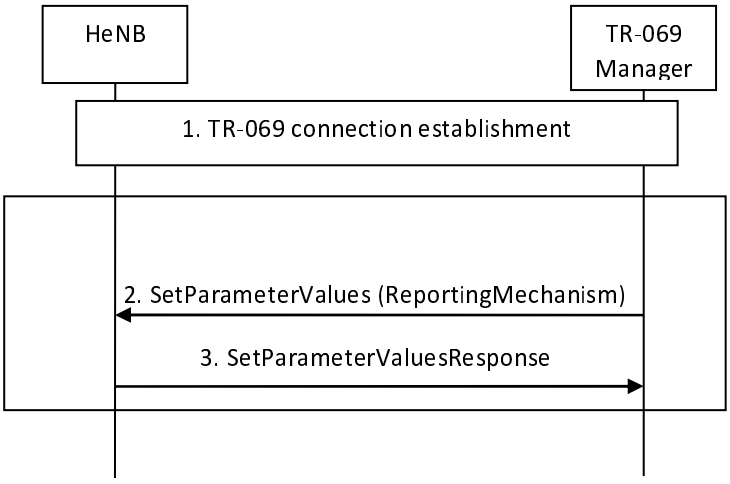


**Figure 5-8: Alarm Reporting Mechanism Configuration**

1. TR-069 connection is established between the HeNB and the HeMS as described in [7].
2. TR-069 Manager initiates the configuration of the alarm reporting mechanism by using SetParameterValues. The parameter ReportingMechanism is defined in [5].

3. HeNB responds to TR-069 Manager by using SetParameterValuesResponse message to indicate success or failure of the procedure. In case of failure the response message returns an error code.

For the details of the SetParameterValues procedure refer to [7] clause A.3.2.1.

### 5.3.2 Alarm reporting procedure for expedited and queued alarms (by RPC method)

When an alarm occurs, the HeNB reports the alarm to the TR-069 Manager using the procedure that depends on the ReportingMechanism of the alarm defined in [5],

This procedure is applicable only to alarms classified as Expedited Handling and Queued Handling with respect to the ReportingMechanism.

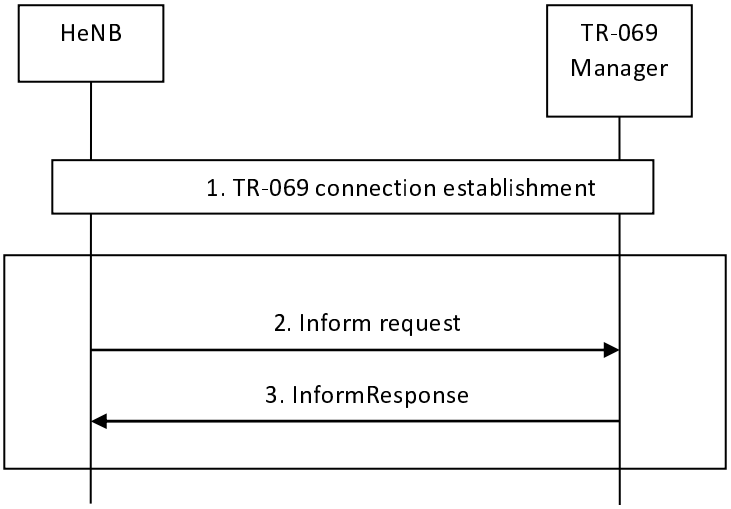


**Figure 5-9: Alarm Reporting Procedure for Expedited and Queued Alarms**

1. A TR-069 connection is established between the HeNB and the HeMS.
2. HeNB reports the alarm directly to TR-069 Manager by using Inform method.
3. When TR-069 Manager receives the alarm, it responds to HeNB with InformResponse message.

For the details of the Inform method refer to [7] clause A.3.3.1.

## 5.4 PM File Upload Procedures

### 5.4.1 PeriodicUploadInterval parameter configuration

TR-069 Manager uses SetParameterValues method to set the PeriodicUploadInterval parameter to define the periodicity for PM file upload. Refer to [5] for definition of the PeriodicUploadInterval parameter.

NOTE: When the PeriodicUploadEnable parameter is set to FALSE - disabled, HeNB shall not initiate PM file upload procedure. Refer to [5] for definition of the PeriodicUploadEnable parameter.

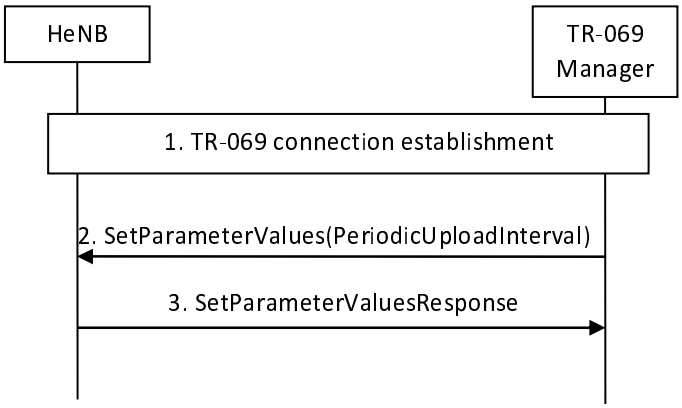


**Figure 5-10: PeriodicUploadInterval parameter configuration**

1. A TR-069 connection is established between the HeMS and the HeNB.
2. TR-069 Manager sets the PeriodicUploadInterval parameter for a PM file upload by the HeNB using SetParameterValues method.
3. HeNB responds to TR-069 Manager by SetParameterValuesResponse to indicate success or failure of the procedure. In case of failure, the HeNB shall return an error code.

NOTE: For details of the SetParameterValues method refer to TR-069 Amendment 2 [7] A.3.2.1

## 5.4.2 PM file upload

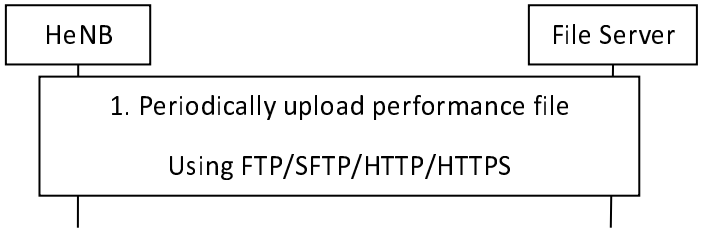


**Figure 5-11: PM file upload**

HeNB uploads the PM file to File Server at every PeriodicUploadInterval (see [5] for parameter definition). The upload method may be one of the following: FTP, SFTP, HTTP, HTTPS (refer to [7] clause A.3.2.2)

# Annex A (informative): Change History

| Change history | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Date** | **TSG #** | **TSG Doc.** | **CR** | **Rev** | **Subject/Comment** | **Old** | **New** |
| Sep 2009 | SA#45 | SP-090552 | -- | -- | Presentation to SA for Information | -- | 1.0.0 |
| Dec 2009 | SA#46 | SP-090738 | -- | -- | Presentation to SA for Approval | 1.0.0 | 2.0.0 |
| Dec 2009 | -- | -- | -- | -- | Publication | 2.0.0 | 9.0.0 |
| Jun 2010 | SA#48 | SP-100264 | 001 | -- | Modify errors in abbreviations and misspelled SSL/TTL in 5.1.2.3. | 9.0.0 | 10.0.0 |
| May 2011 | SA#52 | SP-110288 | 003 | 2 | Correction of procedure flows for HeNB non-IPsec usage - alignment with 33.320 | 10.0.0 | 10.1.0 |
| Sep 2011 | SA#53 | SP-110532 | 007 | 1 | Add the root CA certificate pre-configuration to the discovery procedures | 10.1.0 | 10.2.0 |
| Sep 2011 | SA#53 | SP-110532 | 009 | -- | Add the FQDNs of the Serving SeGW and Serving HeMS to the list of parameters configured by Initial HeMS | 10.1.0 | 10.2.0 |
| Sep 2011 | SA#53 | SP-110634 | 005 | 1 | Editorial cleanup of Serving HeMS Discovery procedure | 10.2.0 | 11.0.0 |
| Jun 2014 | SA#64 | SP-140333 | 010 | 1 | Fix incorrect references to section numbers | 11.0.0 | 12.0.0 |
| 2016-01 | - | - | - | - | Update to Rel-13 version (MCC) | 12.0.0 | 13.0.0 |
| 2017-04 | SA#75 | - | - | - | Promotion to Release 14 without technical change | 13.0.0 | 14.0.0 |
| 2018-06 | - | - | - | - | Update to Rel-15 version (MCC) | 14.0.0 | 15.0.0 |
| 2020-07 | - | - | - | - | Update to Rel-16 version (MCC) | 15.0.0 | 16.0.0 |
| 2022-04 | - | - | - | - | Update to Rel-17 version (MCC) | 16.0.0 | 17.0.0 |
| 2024-04 | - | - | - | - | Update to Rel-18 version (MCC) | 17.0.0 | 18.0.0 |
| 2025-09 | SA#109 | - | - | - | Update to Rel-19 version (MCC) | 18.0.0 | 19.0.0 |

# History

| Document history | | |
|---|---|---|
| V19.0.0 | October 2025 | Publication |
| | | |
| | | |
| | | |
| | | |